游戏公司涉侵犯公民个人信息犯罪的刑法规制与合规应对

作者：杨迅 | 王旭东

摘要：本文聚焦游戏行业数据驱动经营下的刑事合规风险，系统梳理侵犯公民个人信息罪、非法获取计算机信息系统数据罪及帮助信息网络犯罪活动罪的构成要件与实务表现，结合指导性案例与行业实践，深入剖析“用户同意”的阻却效力、公开信息合理利用边界、匿名化与去标识化的动态判断等法律适用疑难问题。针对游戏行业数据流转链条长、参与主体多元、应用场景复杂的特点，文章提出从“制度构建—全流程管控—第三方监督—权限制衡—应急处置”五个维度建立刑事合规体系，强调通过完善内部管理制度阻断单位犯罪认定，依托技术与流程控制消解犯罪构成要件风险，为游戏企业应对高监管环境下的刑事治理挑战提供实务指引。

关键词：游戏公司；公民个人信息；侵犯公民个人信息罪；非法获取计算机信息系统数据罪；帮助信息网络犯罪活动罪；数据合规

近年来，伴随游戏产业高速增长与数据驱动经营的深度耦合，个人信息刑事风险持续攀升。在“增长”“风控”“联运”“营销”等经营目标驱动下，网络游戏经营活动极易异化为非法获取、超范围使用、违规共享乃至黑灰产交易等高风险行为。风险主体亦从传统的黑客、诈骗团伙等外部攻击者，延伸至推广团队、渠道商、SDK 供应商、运营人员等内部关联方，企业本身也可能因制度缺失或默许态度而卷入刑事风险。对依赖实名注册、支付风控、用户画像、买量投放、联运合作等业务模式的游戏企业而言，个人信息已不再只是民事合规议题，而是可能直接触发刑事评价的高敏感业务要素。

如您需要了解我们的出版物，
请联系：

Publication@llinkslaw.com

一. 游戏公司涉个人信息犯罪的主要罪名

近年来，个人信息保护成为各行各业合规的重要关注点之一。事实上，早在 2009 年，严重的买卖个人信息行为即已被纳入刑事规制范围[1]，远早于 2017 年施行的《中华人民共和国网络安全法》和 2021 年施行的《中华人民共和国个人信息保护法》。以刑法手段保护个人信息，为后续数据合规制度奠定了底线。

(一) 侵犯公民个人信息罪

与侵犯个人信息直接对应的罪名，是《中华人民共和国刑法》第二百五十三条之一规定的侵犯公民个人信息罪[2]。该罪是指违反国家有关规定，向他人出售或者提供公民个人信息，或者窃取、以其他方法非法获取公民个人信息，情节严重的行为。自然人和单位均可成为本罪主体；客观方面表现为出售、提供或者非法获取公民个人信息，且达到“情节严重”的程度。该罪经《中华人民共和国刑法修正案(七)》首次设立，并在《中华人民共和国刑法修正案(九)》中完成重要修订：一方面删除了原有的特定主体限制，另一方面增加了“情节特别严重”的量刑档次，并将“违反国家有关规定”纳入构成要件[3]，实现了由“特定主体特殊保护”向“一般主体普遍保护”的转型。

在网络游戏行业实践中，该罪主要体现为以下几类情形：一是数据购买型，例如为买量归因、精准投放而购买玩家手机号、设备号、账号包、实名认证资料；二是违规共享型，例如在联运、广告、客服外包、SDK 接入中，未经有效同意向第三方共享手机号、充值记录、活跃数据和设备信息；三是诱导收集型，例如以礼包、皮肤、返利、代练等名义诱导用户提交验证码、身份证照片、人脸信息或账号密码；四是内部泄露型，例如员工将回流用户包、流失用户标签、实名资料出售给渠道或黑灰产。

(二) 非法获取计算机信息系统数据罪、非法控制计算机信息系统罪

在部分案件中，侵犯公民个人信息还会同时触犯非法获取计算机信息系统数据罪、非法控制计算机信息系统罪。根据《中华人民共和国刑法》第二百八十五条规定，非法获取计算机信息系统数据罪，是指违反国家规定，侵入国家事务、国防建设、尖端科学技术领域以外的计算机信息系统，或者采用其他技术手段，获取该计算机信息系统中存储、处理或者传输的数据，情节严重的行为；非法控制计算机信息系统罪，则是指对前述计算机信息系统实施非法控制，情节严重的行为[4]。两罪共同指向通过技术手段突破系统安全防护措施，非法获取数据或控制系统，且达到“情节严重”标准的行为。

两罪与侵犯公民个人信息罪保护的法益并不相同，前者侧重计算机信息系统安全，后者侧重公民个人信息权益。但在实践中，二者往往形成紧密关联：一方面，二者可能构成手段与目的的

[1] 参见《中华人民共和国刑法修正案(七)》第七条；《中华人民共和国网络安全法》于 2017 年 6 月 1 日起施行；《中华人民共和国个人信息保护法》于 2021 年 11 月 1 日起施行。
[2] 参见《中华人民共和国刑法》第二百五十三条之一。
[3] 参见《中华人民共和国刑法修正案(七)》第七条；《中华人民共和国刑法修正案(九)》第十七条。
[4] 参见《中华人民共和国刑法》第二百八十五条。

牵连关系，行为人往往先通过非法获取计算机信息系统数据或非法控制计算机信息系统作为技术手段获取公民个人信息，进而实施出售或提供行为，在此情形下，司法实践通常按照牵连犯“从一重罪处断”的思路处理，也可能结合具体案情实行数罪并罚；另一方面，侵犯个人信息的结果本身，也可能成为认定第二百八十五条所称“情节严重”的依据，例如获取非金融类身份认证信息五百组以上，即可能达到入罪门槛[5]。

在游戏行业，此类犯罪常见于：利用游戏客户端或服务端接口漏洞抓取玩家信息；通过撞库获取账号密码；利用木马或后门控制玩家后台设备；越权访问或导出用户数据库；开发或使用爬虫程序非法获取游戏内公开但仍受保护的玩家数据等。

(三) 帮助信息网络犯罪活动罪

在一些情况下，行为人虽然没有直接实施侵犯公民个人信息行为，但如果为该类行为提供帮助，也可能构成帮助信息网络犯罪活动罪(以下简称“帮信罪”)。《中华人民共和国刑法》第二百八十七条之二规定的帮信罪，是指明知他人利用信息网络实施犯罪，而为其提供互联网接入、服务器托管、网络存储、通信传输等技术支持，或者提供广告推广、支付结算等帮助，情节严重的行为[6]。该罪的核心构成要件，集中体现为“明知”与“帮助行为”两个方面：前者决定行为人的主观心态，后者界定行为性质及其与下游犯罪之间的连接强度。

需要注意的是，帮信罪虽为信息网络犯罪提供帮助，但并不当然等同于相关犯罪的共犯。共犯要求对具体犯罪具有共同故意，而帮信罪并不要求行为人对利用信息网络实施的下游犯罪具有完整、具体的认识。以帮助侵犯公民个人信息为例，帮信罪的成立并不要求行为人明确知悉下游具体侵犯了哪些个人信息、采取了何种具体手段；只要其明知自己所提供的信息网络服务已成为侵犯公民个人信息犯罪链条中的一环，仍然提供相应支持，即可能成立本罪。

在游戏行业中，帮信罪主要体现为：为黑灰产提供实名账号池、自动切换网络地址系统、批量接收短信或语音验证码平台；明知他人从事游戏诈骗、赌博、洗钱等犯罪，仍提供广告导流、支付结算、接口能力或批量注册工具；将游戏账号、验证码平台等提供给下游犯罪使用等。当实名账号、社交账号、验证码、批量注册工具被持续输送给诈骗、洗钱、赌博、引流黑产，且下游用途明显违法时，提供者便很难再以“增长服务”“卖号”或“技术支持”进行抗辩。

二. 法律适用中的前沿问题与疑难争点

刑法中“公民个人信息”的概念边界相对模糊，司法上主要依赖《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》(下称《侵犯公民个人信息罪解释》)进行界定[7]。《中华人民共和国个人信息保护法》作为后出台的综合性立法，对个人信息保护提出了更系

[5] 参见《最高人民法院、最高人民检察院关于办理危害计算机信息系统安全刑事案件应用法律若干问题的解释》(法释〔2011〕19 号)第一条、第十一条。
[6] 参见《中华人民共和国刑法》第二百八十七条之二。
[7] 参见《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》(法释〔2017〕10 号)。

统、更宽泛的规范要求。在司法实践中，可以参考《个人信息保护法》理解刑法概念，但并不意味着刑法评价应完全等同于民事、行政法意义上的个人信息范围。

(一) 游戏账号、行为数据与设备标识的个人信息属性

刑法层面，根据《侵犯公民个人信息罪解释》第一条，公民个人信息是指“以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息”[8]。最高人民法院第 35 批指导性案例对此作了重要阐释：指导性案例 193 号明确，居民身份证信息中包含姓名、人脸识别信息、身份号码、户籍地址等多种个人信息，整体上属于可能影响人身、财产安全的敏感信息[9]；指导性案例 194 号则指出，微信号等社交媒体账号因与手机号、银行卡等绑定，并兼具社交、支付功能，可以认定为公民个人信息[10]。

与此相比，《个人信息保护法》第四条对个人信息作出了更广义的界定，即“以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息”[11]。刑法与个保法虽然都使用“个人信息”这一概念，但规范目的并不完全相同：前者作为制裁法，强调构成要件的明确性，防止刑罚边界过度扩张；后者作为数字时代的综合性立法，则需要覆盖更广泛、更复杂的数据处理场景。因此，在刑法评价上，更容易被纳入规制范围的，通常是识别度较高、关联性较强、敏感性更高的信息。

在游戏行业实践中，涉及的主要个人信息类型包括：一是身份标识类，如实名认证的姓名、身份证号、手机号；二是网络身份类，如游戏账号、UID、IP 地址、设备 MAC 地址、IMEI 等；三是行为数据类，如登录日志、游戏时长、充值记录、消费习惯、社交关系、战绩数据、位置轨迹等。对平台运营方而言，看似匿名的 UID 在后台往往可与特定自然人关联，判断重点并不在于字段名称，而在于其识别性、可关联性与活动反映性。

(二) “用户同意”能否阻却犯罪

获取、使用、提供、转移公民个人信息，即便在收集阶段取得了相关用户的同意，也并不必然阻却个人信息犯罪的成立。换言之，经用户同意而收集的个人信息，后续如被非法获取、使用、提供或者转移，仍然可能触发刑事评价。

我国刑法并未明确规定“用户同意”能否阻却犯罪，因此相关行为的合法性判断，需要结合《个人信息保护法》的规范体系加以分析。根据该法，个人信息处理应当遵循合法、正当、必要和诚信原则；“同意”只是个人信息处理的合法性基础之一，并不当然证明处理行为具有正当性与必要性[12]。其中，正当性要求处理者具有真实、明确且合法的处理目的，不得以欺诈、胁迫等方式处理个人信息；必要性则要求处理范围与处理目的保持一致，不得超出同意范围。因此，即

[8] 同上注，第 1 条。
[9] 参见最高人民法院指导性案例 193 号“闻巍等侵犯公民个人信息案”。
[10] 参见最高人民法院指导性案例 194 号“熊昌恒等侵犯公民个人信息案”。
[11] 参见《中华人民共和国个人信息保护法》第四条。
[12] 参见《中华人民共和国个人信息保护法》第五条、第六条、第十三条。

便用户曾经作出同意，只要该同意系在误导、胁迫等情形下作出，或者后续处理明显超出原有授权范围，该处理行为仍可能被认定为非法。

在游戏场景中，同意机制的瑕疵通常表现为以下三类：一是捆绑式同意，将“游戏运行所必需”的授权与“广告推荐、画像分析、联合营销、第三方共享”等非必要处理混为一谈；二是超越同意目的范围，玩家仅同意将信息用于注册、登录和支付安全，企业却将其用于广告画像、交叉营销；三是同意链条断裂，例如向第三方 SDK 共享数据时，未就共享行为单独征得用户同意。其中，前述第一类情形与《个人信息保护法》第十六条关于“不得因个人不同意处理其个人信息或者撤回同意，拒绝提供产品或者服务”的规定存在直接张力[13]。刑事司法并不会因为企业“有协议、有勾选、有页面”就当然认定已经取得有效授权；若处理行为明显超出合理范围或者具有欺骗性，即便表面上存在同意，也未必能够阻却犯罪。

(三) “已公开信息”抓取与二次利用的边界

对已经公开的个人信息进行处理，并不当然具有合法性。

我国刑法并未明确规定侵犯公民个人信息犯罪的对象是否可以包括公开信息，但这一问题可以借助《个人信息保护法》的规范进行解释。该法第二十七条规定，个人信息处理者可以在合理范围内处理个人自行公开或者其他已经合法公开的个人信息；个人明确拒绝的除外[14]。此处所谓“合理范围”，通常应理解为与个人公开信息时的目的、场景和预期用途保持一致。例如，用户在公开游戏排行榜中展示昵称和战绩，其主要目的通常是在游戏社区内部展示成就，而非供第三方用于商业营销或精准诈骗。

在游戏行业中，超出合理范围使用公开信息的常见情形包括：从公开页面抓取用户名单、评论信息、高战力账号名单，再用于博彩推广、代练服务、高风险营销或者撞库攻击；将公开渠道获取的玩家数据与其他渠道数据进行汇聚融合，以重新识别特定个人；改变公开信息原有用途，例如将原本用于游戏内匹配的地理位置信息转用于线下追踪等。对此，指导性案例 194 号已明确指出，未经本人同意或者不具备法律授权等法定理由，通过购买、收受、交换等方式获取在一定范围内已公开的公民个人信息后进行非法利用，改变其原有范围、目的和用途的，不属于合理处理[15]。

(四) 匿名化、去标识化与可回识别能力的判断

对“脱敏”后的个人信息进行处理，是否仍可能构成侵犯公民个人信息犯罪，是实务中争议较大的问题。

“脱敏”并非严格的法律术语。在个人信息保护法体系下，常见的对应概念是“匿名化”与“去标识化”。《个人信息保护法》第七十三条明确区分二者：匿名化，是指个人信息经过处理后无法识别特定自然人且不能复原的过程；去标识化，是指个人信息经过处理后，在不借助额外信息的

[13] 参见《中华人民共和国个人信息保护法》第十六条。
[14] 参见《中华人民共和国个人信息保护法》第二十七条。
[15] 参见最高人民法院指导性案例 194 号“熊昌恒等侵犯公民个人信息案”。

情况下无法识别特定自然人的过程[16]。理论上，匿名化后的信息不再属于个人信息；而去标识化只是降低识别风险的安全措施，并不改变信息仍属个人信息的法律属性。

然而在实践中，匿名化与去标识化并非泾渭分明。所谓“匿名化”也并非绝对不可还原，其判定不仅取决于技术手段(如差分隐私、K-匿名、同态加密)，还取决于管理措施(如密钥分离、访问隔离)以及现实法律环境(如重识别是否被禁止或事实上难以实现)。因此，在刑法意义上，脱敏处理无论采取匿名化还是去标识化路径，都只能在一定程度上降低刑事责任风险，而不能绝对阻却侵犯公民个人信息犯罪的成立。

在游戏企业实践中，常见的“脱敏数据”往往只是删除姓名、掩码手机号、替换为 UID 或进行哈希处理，但后台仍保留映射表、设备指纹、行为特征或支付链路。在此路径下，相关信息通常仅完成了简单的去标识化，远未达到匿名化程度。若通过撞库，或者结合其他外部信息仍可重新识别特定个人，则所谓“匿名化”即告失效。例如，将玩家游戏行为数据(如特定时段的登录规律、消费模式)与其他数据源结合，可能精准定位到特定个人；对用户进行细分标签(如“高净值北京海淀玩家”)，当标签组合足够细时，同样可能实现重识别。一旦侦查机关能够证明该类数据在企业控制范围内具备可识别能力，企业便难以单纯以“已经脱敏”为由免责。

三. 刑事证明的主要难点及其应对

由于个人信息具有无形性，且在实践中流转链条复杂，判断侵犯个人信息犯罪的行为并不容易。

(一) 侵犯个人信息数量的认定

侵犯个人信息的数量，是判断是否构成犯罪以及量刑档次的关键尺度。根据《侵犯公民个人信息罪解释》第五条第(三)项至第(六)项规定，非法获取、出售或者提供公民个人信息的，依据所涉信息的性质和种类，分别适用五十条、五百条和五千条三档数量标准；单项或者按比例综合达到相应标准的，即可认定为“情节严重”[17]。

在互联网游戏行业，判定侵犯公民个人信息数量的困难主要在于：游戏数据结构复杂，手机号、昵称、设备号、充值段位、活跃标签、战力数据、登录时间等信息往往混合于同一数据表，且字段可能存在重复、缺失、错码或嵌套；相关数据还可能分散在日志、缓存、备份、测试库等多个系统中，去重和真伪鉴别均存在较高技术难度。对此，司法实践通常采取以下思路：允许按照查获数量直接认定，但明确不真实或者重复的信息应予剔除；非法获取后又出售、提供的，条数原则上不重复计算，但向不同对象重复出售同一信息的，则应累计计算；必要时可以委托专业机构出具技术鉴定意见，完成数据清洗、去重和字段分类。

[16] 参见《中华人民共和国个人信息保护法》第七十三条。
[17] 参见《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》(法释〔2017〕10 号)第五条。

(二) 个人信息非法来源的认定

处理的个人信息是否具有合法来源，是区分罪与非罪的重要依据。判断规则上，需要审查数据获取是否违反国家有关规定，是否未经同意或者超越授权范围。实践中，大量案件并非典型的黑客窃取，而是被包装成渠道回传、SDK 共享、联运导流、客服外包、买量归因等“正常商业合作”，由此形成“形式合法、实质非法”的复杂局面。

尤其在网络游戏相关案件中，数据流转链条长、中间环节多、源头追溯困难；授权文件可能形式完备但实质失真，例如用户系在误导下点击同意；多层转卖后还可能发生证据链断裂。实践中的认定通常包括：审查数据流转的完整链条，从数据源头追溯到最终使用环节；核查授权同意的真实性、明确性与范围；对于无法说明合法来源的数据，结合交易价格、交易方式、数据敏感程度等因素推定其来源非法；要求企业对数据合法性承担说明和举证责任，不能说明或者说明不足时，需承担相应不利后果。

(三) 主观恶意的判断

侵犯公民个人信息罪属于故意犯罪，要求行为人明知自己的行为会导致侵犯公民个人信息的结果，并希望或者放任该结果发生。但是，游戏行业中的许多高风险行为常常披着“增长”“召回”“反作弊”“运营支撑”的外衣，技术中立与主观恶意之间的边界较为模糊；行为人的“明知”也往往表现为间接故意或推定明知，难以直接证明。

司法实践中，通常通过客观行为反推主观故意。例如，企业要求用户交付验证码、身份证照片、面部信息，本身即反映其对信息敏感性的认知；使用代理 IP、自动切换网络地址、批量账号、验证码平台，反映其具有规避监管的意图；设置“免费皮肤”“返利礼包”“代领福利”等诱导性话术，反映其主动获取信息的目的；交易价格明显偏离市场价格、在异常时段交易、使用隐蔽通信工具等，也均可作为推定非法意图的重要事实。

(四) 区分个人行为和单位行为

个人和公司都可能成为侵犯公民个人信息犯罪的主体。区分个人行为与单位行为，关系到单位犯罪与个人犯罪的认定。单位犯罪要求体现单位意志、为单位利益、以单位名义实施。实践中，如果违规数据处理是在公司制度、业务目标、岗位分工和收益归集框架内持续发生，即便具体操作由员工完成，也可能被认定为单位犯罪；反之，如果系员工个人私自实施、利益归个人所有、明显违反公司制度，则更可能被认定为个人犯罪。

区分的难点在于：游戏企业常将数据获取、买量等业务外包或交由具体团队执行，KPI 设计、激励机制可能间接鼓励违规行为，如何认定“单位意志”因而存在较大争议。实践中，侦查机关通常会从 KPI 设计、激励机制、业务模式、审批流程和收益归集路径等因素反向推定公司是否具有组织性、容忍性乃至决策性。公司能否证明自己已经设置合法边界、实施过审核、反对相关做法并及时纠正异常行为，往往直接影响单位责任与个人责任的切分。

四. 减小刑事风险的合规建议

个人信息保护的合规建设，不仅是减少个人信息违法处理、减轻行政或民事责任的重要途径，更是企业阻断刑事归责、争取“出罪”或者“降格”处理的关键防线。对企业而言：一方面，应通过建立完善的制度体系，证明企业不具备犯罪的主观故意，避免因员工个人行为被认定为单位犯罪；另一方面，应通过技术控制和管理流程，实质性消除或降低侵犯公民个人信息罪、非法获取计算机信息系统数据罪及帮信罪等罪名的构成要件风险。

(一) 建立和完善企业个人信息保护管理制度

依据《个人信息保护法》的要求建立和完善个人信息保护管理制度，不仅是个保法意义上的合规要求，也是降低个人信息犯罪刑事风险的重要保障。

企业是否建立完善的内部管理制度，是区分单位犯罪与个人犯罪、判断企业是否具有主观故意的重要依据。若企业未制定个人信息保护的基本规章制度，或者制度形同虚设，可能被司法机关认定为对数据违法行为存在默许、放任乃至决策性支持，从而触发单位犯罪认定；反之，完备的制度体系则有助于证明企业已经设置合法边界，在发生员工个人犯罪时，可作为切分单位责任与个人责任的重要抗辩事实。

就制度建设而言，网络游戏企业应依据《个人信息保护法》第五十一条第一款制定内部管理制度和操作规程，明确个人信息保护负责人；进一步还可参照《企业个人信息安全管理规范》(T/SIA 001-2022)第 7.3.1 条，建立覆盖个人信息管理机构及职责、安全风险管理、处理活动管理、设备设施安全管理、数据库管理、文档管理、宣传培训、内审、持续改进、事件应急及违规处罚等方面的基本管理规定[18]。通过制度化建设，将“目的明确”“最小必要”等原则嵌入业务流程，能够有效避免因系统性违规而触发刑事风险。

(二) 开展个人信息闭环管理与全流程安全控制

加强个人信息保护合规、降低个人信息犯罪刑事风险，不能仅依赖高层级的管理制度，更重要的是在个人信息处理各环节加强监控，实施全流程安全控制。

侵犯公民个人信息罪的成立，往往源于处理环节失控：超范围收集可能构成“非法获取”，违规使用可能构成“非法提供”，保存不当导致泄露还可能成为量刑加重情节。实施全生命周期闭环管理，能够在各处理环节设置“阻断点”，确保数据处理始终处于合法、正当、必要的轨道之上，从而消除犯罪构成要件中的“非法性”基础。

互联网游戏企业可以参照《企业个人信息安全管理规范》第 8 部分“处理过程”的要求，建立覆盖收集、存储、使用、转移、销毁等环节的全流程控制[19]：在收集环节严格遵循合法目的与最

[18] 参见《中华人民共和国个人信息保护法》第五十一条第一款；《企业个人信息安全管理规范》(T/SIA 001-2022)第 7.3.1 条。
[19] 参见《企业个人信息安全管理规范》(T/SIA 001-2022)第 8 部分。

小必要原则，禁止欺诈、诱骗收集；在存储环节实施分类管理与加密脱敏，确保个人敏感信息与一般信息隔离存储；在使用环节建立严格的授权审批与日志审计，防止越权访问与非法导出；在转移环节进行个人信息保护影响评估并审查接收方资质；在后处理环节，对超期数据实施彻底销毁或匿名化。通过闭环管理，能够确保任何个人信息处理均可追溯、可控制、可终止。

(三) 第三方供应商管理

在个人信息处理各环节中，不安全、不可靠的第三方供应商，可能给企业带来难以预测的合规与刑事风险。以游戏行业为例，联运方、SDK 提供商、买量代理等第三方往往是数据泄露和非法流转的高风险节点。若第三方利用企业提供的数据实施侵犯公民个人信息犯罪或帮信罪，企业可能因未尽合理注意义务而被认定为共犯，或者因“明知”他人利用信息网络实施犯罪而构成帮信罪。通过全过程管理，企业可以证明自己已经履行合理审慎义务，阻断“明知”或“应知”的刑事推定。

因此，当企业将个人信息委托第三方处理时，应依照法律要求开展事前尽调、事中监督和事后回顾。具体而言，依据《个人信息保护法》第二十一条，企业应对受托处理人实施严格监督；同时可参照《信息安全技术 个人信息安全规范》(GB/T 35273-2020)，对受托方进行尽职调查与能力评估，签订明确处理目的、范围、期限、权利义务及再委托限制的合同；在处理过程中建立审计与技术检测机制，确保受托方行为符合约定；合作结束后，监督其及时删除个人信息并保留记录[20]。对于来源不明的数据接入，应实行“一票否决”，避免企业自身成为黑灰产数据流转链条中的一环。

(四) 落实最小必要与分权制衡的内部权限管控

内部人员越权访问、批量导出、私自截屏保存数据，是游戏行业侵犯公民个人信息犯罪的重要表现形式。通过严格的访问控制与权限分离，一方面可以预防员工个人实施非法获取、出售个人信息；另一方面，在发生内部人员违法犯罪时，企业也可通过完善的权限记录与审批日志证明该行为违反公司制度、超越授权范围，从而说明其属于个人犯罪而非单位犯罪，或者证明企业已尽到安全管理义务，不应承担相应刑事责任。

《个人信息保护法》以及《信息安全技术 个人信息安全规范》为信息系统内部权限管理提供了基本原则。据此，企业至少应建立以下机制：落实最小授权原则，确保员工仅能访问职责所需的最小必要信息；对批量查询、导出、修改等重要操作设置双人审批与异常告警；对安全管理人员、数据操作人员、审计人员实行角色分离；确需超权限处理的，应由个人信息保护负责人审批并留痕；建立离职、转岗场景下的权限即时回收机制[21]。通过技术手段实现“谁能看、谁能导、何时导”的全流程可控，方能有效堵住“内部人风险”。

[20] 参见《中华人民共和国个人信息保护法》第二十一条；《信息安全技术 个人信息安全规范》(GB/T 35273-2020)。
[21] 参见《中华人民共和国个人信息保护法》第五十一条；《信息安全技术 个人信息安全规范》(GB/T 35273-2020)。

(五) 建立和实施应急预案，将损失控制在最低程度

及时、有效的应急处置，不仅属于民事与行政法上的减损义务，也是刑事量刑中具有现实意义的重要考量因素。根据《侵犯公民个人信息罪解释》，“情节严重”或者“情节特别严重”的认定，往往与信息泄露后的扩散范围和危害后果直接相关；行为人若能及时采取补救措施、防止损害扩大，可能避免达到更高量刑档次。同时，初犯、全部退赃并具有悔罪表现的行为人，在不属于“情节特别严重”的情况下，也可能适用从宽处理规则[22]。

《个人信息保护法》及相关配套规则也为企业建立应急预案提供了基本框架。预案一般应包括：应急响应组织架构与职责分工；事件分级标准(特别重大、重大、较大、一般)；事件发现、报告与处置流程；向监管部门报告以及向个人信息主体告知的机制；证据保全与系统恢复措施等。企业应定期组织应急演练，确保在发生个人信息泄露、篡改、丢失时，能够迅速启动“先留证再封堵、先固定再清理”的处置流程，及时履行报告义务，最大限度降低损害后果和刑事风险。

[22] 参见《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》(法释〔2017〕10 号)第五条、第十条。

如您希望就相关问题进一步交流，请联系：

杨迅
+86 21 3135 8799
xun.yang@llinkslaw.com

王旭东
+86 755 3391 7631
edward.wang@llinkslaw.com

如您希望就其他问题进一步交流或有其他业务咨询需求，请随时与我们联系：**master@llinkslaw.com**

上海	北京	深圳
上海市银城中路 68 号 时代金融中心 19 楼 T: +86 21 3135 8666 F: +86 21 3135 8600	北京市朝阳区光华东里 8 号 中海广场中楼 30 层 T: +86 10 5081 3888 F: +86 10 5081 3866	深圳市南山区科苑南路 2666 号 中国华润大厦 18 楼 T: +86 755 3391 7666 F: +86 755 3391 7668
香港	**伦敦**	
香港中环遮打道 18 号 历山大厦 32 楼 3201 室 T: +852 2592 1978 F: +852 2868 0883	1/F, 3 More London Riverside London SE1 2RE T: +44 (0)20 3283 4337 D: +44 (0)20 3283 4323	

www.llinkslaw.com

Wechat: LlinksLaw

本土化资源 国际化视野